AL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,644	10/15/2003	Steven L. Teixeira	VIV/0012.01	2643

28653 7590 01/23/2008
JOHN A. SMART
708 BLOSSOM HILL RD., #201
LOS GATOS, CA 95032

EXAMINER	
LASHLEY, LAUREL L	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:. 10/605,644
Filing Date: October 15, 2003
Appellant(s): TEIXEIRA, STEVEN L.

John A. Smart
Registration No. 34,929
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/13/2007 appealing from the Office action mailed 06/11/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US Patent Publication No. 2004/0162808	Margolus, et al.	08-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

Claims 1 – 55 are rejected under 35 U.S.C. 102(e) as being anticipated by Margolus et al in US Patent Application Publication No. 2004/0162808 (hereinafter US PGPub '808).

As for claim 1, US PGPub '808 discloses:

In a computer system, a method for protecting sensitive information, the method comprising:

receiving input of sensitive information from a user;

computing a data shadow of the sensitive information for storage in a repository, and thereafter discarding the input so that the sensitive information itself is not stored;

based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and

blocking any detected attempt to transmit the sensitive information that is not authorized by the user. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 2, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises structured data. (see [0054], lines 3 – 9)

For claim 3, US PGPub '808 discloses:

The method of claim 2, wherein said data shadow is computed for the structured data as a regular expression and a hash. (see [0010], lines 4 – 9)

For claim 4, US PGPub '808 discloses:

The method of claim 3, wherein said hash comprises a MD-5 hash. (see [0059])

For claim 5, US PGPub '808 discloses:

The method of claim 2, wherein said structured data includes credit card number information. (see [0051], lines 4 –6; [0054], lines 3-9)

For claim 6, US PGPub '808 discloses:

The method of claim 2, wherein said structured data includes Social Security number information. (see [0051], lines 4 – 6; [0054], lines 3 – 9)

For claim 7, US PGPub '808 discloses:

The method of claim 3, wherein said regular expression represents formatting information for said structured data. (see 0054], lines 3 – 9)

For claim 8, US PGPub '808 discloses:

The method of claim 3, wherein said hash is computed after normalization of the structured data. (see [0054], lines 3 – 9)

For claim 9, US PGPub '808 discloses:

The method of claim 8, wherein said normalization includes removing any formatting information before computing the hash. (see [0059])

For claim 10, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises structured data and said detecting step includes: initially detecting said structured data by matching a format for that structured data. (see [0054], lines 3 – 9)

For claim 11, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises literal data. (see [0054], lines 3 – 9)

For claim 12, US PGPub ‘808 discloses:

The method of claim 11, wherein said data shadow is computed for the literal data as a length value plus at least one hash of the literal data. (see [0010], lines 4 – 9)

For claim 13, US PGPub ‘808 discloses:

The method of claim 12, wherein said at least one hash includes an additional first pass hash or checksum value computed for the literal data. (see Figure 5 & 6)

For claim 14, US PGPub ‘808 discloses:

The method of claim 12, wherein said at least one hash includes a MD-5 hash computed for the literal data. (see [0059])

For claim 15, US PGPub ‘808 discloses:

The method of claim 1, wherein said at least one hash includes an optional checksum value computed for the literal data that allows relatively quick detection of the sensitive information and a MD-5 hash that allows subsequent verification. (see [0059]; [0066], lines 3 – 14)

For claim 16, US PGPub ‘808 discloses:

The method of claim 1, wherein said receiving input step includes: receiving input indicating a type for the sensitive information. (see [0054], lines 3 – 9)

For claim 17, US PGPub ‘808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a password. (see [0051])

For claim 18, US PGPub ‘808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a Social Security number. (see [0051])

For claim 19, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a credit card number. (see [0051])

For claim 20, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a personal identification number (PIN). (see [0051])

For claim 21, US PGPub '808 discloses:

The method of claim 1, further comprising: automatically determining a type for the sensitive information that indicates formatting. (see [0054]; [0062])

For claim 22, US PGPub '808 discloses:

The method of claim 21, wherein said step of automatically determining a type includes: matching the input against a template for identifying a type. (see [0051])

For claim 23, US PGPub '808 discloses:

The method of claim 1, wherein said detecting step includes: trapping an outbound buffer of data that may contain the sensitive information; and in instances where the sensitive information comprises structured data, performing a regular expression search on the outbound buffer. (see [0011]; [0064] - [0065]; Figure 5)

For claim 24, US PGPub '808 discloses:

The method of claim 23, further comprising: if a regular expression match is found, normalizing data from the match so as to remove formatting and thereafter computing a hash on it, for comparison with corresponding hash values stored in the repository. (see [0011])

For claim 25, US PGPub '808 discloses:

The method of claim 24, wherein said hash is a MD-5 hash. (see [0059])

For claim 26, US PGPub '808 discloses:

The method of claim 1, wherein said detecting step includes: trapping an outbound buffer of data that may contain the sensitive information; and in instances where the sensitive information comprises literal data, performing a sliding window search on the outbound buffer. (see Figure 5)

For claim 27, US PGPub '808 discloses:

The method of claim 26, wherein said sliding window search includes performing an optional checksum calculation on successive blocks of bytes within the outbound buffer, for comparison with corresponding checksum values stored in the repository. ([0011]; [0064]-[0065]; Figure 5)

For claim 28, US PGPub '808 discloses:

The method of claim 27, further comprising: if a match is found based on the checksum comparison, verifying the match with a MD-5 hash performed on data from the match. (see [0011]; [0048])

For claim 29, US PGPub '808 discloses:

The method of claim 28, wherein said MD-5 hash performed on data from the match is compared against a corresponding MD-5 hash value stored in the repository. (see [0011])

For claim 30, US PGPub '808 discloses:

The method of claim 1, wherein said step of blocking includes: referencing a stored policy indicating whether the sensitive information should be blocked from transmission. ([0012], lines 4-11)

For claim 31, US PGPub '808 discloses:

A computer-readable medium having processor-executable instructions for performing the method of claim 1. (see Abstract; Figures 1 – 10)

For claim 32, US PGPub '808 discloses:

A downloadable set of processor-executable instructions for performing the method of claim 1. (see Abstract; Figures 1 – 10)

As for claim 33, US PGPub '808 discloses:

In a computer system, a method for securing sensitive items from inappropriate access, the method comprising:

receiving input from a user indicating that a particular sensitive item is to be protected from inappropriate access;

storing metadata characterizing the particular sensitive item, and thereafter discarding the input so that the particular sensitive item itself is not stored;

based on the stored metadata, detecting whether the particular sensitive item is present in any transmission of outgoing data; and

trapping any transmission of outgoing data that is detected to contain the particular sensitive item. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 34, US PGPub '808 discloses:

The method of claim 33, further comprising: a policy indicating what action the system should be taken upon trapping transmission of outgoing data that contains the particular sensitive item. (see [0011])

For claim 35, US PGPub '808 discloses:

The method of claim 34, wherein said action includes blocking any trapped transmission. (see [0012], lines 4 – 11)

For claim 36, US PGPub '808 discloses:

The method of claim 34, wherein said action includes querying the user about whether the particular sensitive item may be transmitted. (see [0011], [0012], lines 4 – 11; [0013])

For claim 37, US PGPub '808 discloses:

The method of claim 33,.wherein said metadata includes a one-way hash of the particular sensitive item. (see [0059])

For claim 38, US PGPub '808 discloses:

The method of claim 37, wherein said one-way hash comprises a MD-5 hash. (see [0059])

For claim 39, US PGPub '808 discloses:

The method of claim 33, wherein said particular sensitive item comprises structured data, and wherein said metadata includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data. (see [0059])

For claim 40, US PGPub '808 discloses:

The method of claim 39, wherein said trapping step includes: locating the particular sensitive item by first performing a regular expression search on the outgoing data for finding a match based on formatting; and for any match found based on formatting, performing a hash on the match to determine whether it matches a corresponding hash stored as part of the metadata. (see [0059])

For claim 41, US PGPub '808 discloses:

The method of claim 33, wherein said particular sensitive item comprises literal data and wherein said metadata comprises as a length value plus at least one hash of the literal data. (see [0054], lines 3 - 9)

For claim 42, US PGPub '808 discloses:

The method of claim 41, wherein said trapping step includes: locating the particular sensitive item by first performing a sliding window search through the outgoing data for a block of bytes having a size equal to said length value and having a hash value equal to one of said at least one hash of the literal data. (see [0011]; [0064] – [0065]; Figure 5)

For claim 43, US PGPub ‘808 discloses:

The method of claim 42, wherein said at least one hash includes a MD-5 message digest computation. (see [0059])

For claim 44, US PGPub ‘808 discloses:

The method of claim 43, wherein said at least one hash further includes an optional first pass hash or checksum as an optimization. (see Figure 5 & 6)

For claim 45, US PGPub ‘808 discloses:

A computer-readable medium having processor-executable instructions for performing the method of claim 33. (see Abstract; Figures 1 – 10)

For claim 46, US PGPub ‘808 discloses:

A downloadable set of processor-executable instructions for performing the method of claim 33. (see Abstract; Figures 1 – 10)

As for claim 47, US PGPub ‘808 discloses:

A system providing security for sensitive information, the system comprising:

a data processing system receiving input of sensitive information;

a secure lockbox module for storing a secure descriptor characterizing the sensitive information, so that the system can detect transmission of the sensitive information without a copy of the sensitive information itself being stored; and a security module for detecting, based on said secure descriptor, any attempted transmission of outgoing data that contains the sensitive information. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 48, US PGPub ‘808 discloses:

The system of claim 47, wherein said input includes an indication of a type for the sensitive information. (see [0054], lines 3 –9)

For claim 49, US PGPub ‘808 discloses:

The system of claim 48, wherein said indication of a type includes a selected one of structured data and literal data. (see [0054], lines 3 – 9)

For claim 50, US PGPub ‘808 discloses:

The system of claim 49, wherein said structured data includes a credit card number. (see [0051])

For claim 51, US PGPub ‘808 discloses:

The system of claim 47, further comprising: a security policy specifying what action is to be undertaken when the security module detects an attempt to transmit the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 52, US PGPub ‘808 discloses:

The system of claim 51, wherein said security policy specifies an action of blocking any attempted transmission of the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 53, US PGPub ‘808 discloses:

The system of claim 51, wherein said security policy specifies an action of prompting a user to allow or deny any attempted transmission of the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 54, US PGPub ‘808 discloses:

The system of claim 47, wherein said sensitive information includes structured data, and wherein said secure descriptor includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data. (see [0054]; [0059])

For claim 55, US PGPub '808 discloses:

The system of claim 47, wherein said sensitive information includes literal data and wherein said secure descriptor includes a length value plus at least one hash of the literal data. (see [0054]; [0059])

(10) Response to Argument

A. Claim 1-55, primarily Claim 1

In the present case, the Appellant argues that Margolus does not disclose an improved lockbox that stores data "shadows," so that the underlying sensitive information itself never need be stored.

With regard to this argument, the Examiner believes Margolus et al. teaches that a data-item is deposited if a data-name, which is a digitally fingerprinted data-item, is not already in the data repository (see Figure 1). Margolus et al. teaches that digitally fingerprinted data-item (i.e. the data-name) is stored in the repository and not the actual data-item (see [0011], lines 2 – 6: comparison of digital fingerprints of the data items; [0059]-[0060]: depositing and retrieving stored digitally fingerprinted data-item in repository). In short, it is Margolus' data-name that is stored in the repository, not the data-item. Like Appellant's claimed invention, Margolus teaches that data-items (sensitive information) are never stored (see [0011]: lines 9-11: data items are always encrypted prior to transmission to storage device). As such, Margolus' disclosure satisfies Appellant's claim limitation of unstored sensitive information.

Accordingly, for reasons discussed above, the Examiner maintains that Margolus teaches the elements of claim 1 and therefore the rejection is maintained for claims 1 -55.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Laurel Lashley
Examiner, GAU 2132
14 January 2008

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron, Jr.
Supervisory Patent Examiner, GAU 2132

Benjamin Lanier
Primary Examiner, GAU 2132